



DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 5

[Docket No. ICEB-2020-0007]

Privacy Act of 1974: Implementation of Exemptions; U.S. Department of Homeland Security/Immigration and Customs Enforcement-018 Analytical Records System of Records

AGENCY: U.S. Immigration and Customs Enforcement, U.S. Department of Homeland Security.

ACTION: Notice of proposed rulemaking.

SUMMARY: The U.S. Department of Homeland Security (DHS) is giving concurrent notice of a newly established system of records pursuant to the Privacy Act of 1974 for the “DHS/U.S. Immigration and Customs Enforcement (ICE)-018 Analytical Records System of Records” and this proposed rulemaking. In this proposed rulemaking, the Department proposes to exempt portions of the system of records from one or more provisions of the Privacy Act because of criminal, civil, and administrative enforcement requirements.

DATES: Comments must be received on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number ICEB-2020-0007, by one of the following methods:

- Federal e-Rulemaking Portal: <http://www.regulations.gov>. Follow the instructions for submitting comments.
- Fax: 202-343-4010.

- Mail: James Holzer, Acting Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

Instructions: All submissions received must include the agency name and docket number for this notice. All comments received will be posted without change to

<http://www.regulations.gov>, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to <http://www.regulations.gov>.

FOR FURTHER INFORMATION CONTACT: For general questions please contact:

Jordan Holz, ICEPrivacy-GeneralMailbox@ice.dhs.gov, Privacy Officer, U.S.

Immigration and Customs Enforcement (ICE), 500 12th Street SW, Mail Stop 5004,

Washington, D.C. 20536. For privacy questions, please contact: James Holzer,

Privacy@hq.dhs.gov, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, U.S.

Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background:

In accordance with the Privacy Act of 1974, 5 U.S.C. sec. 552a, the U.S. Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE) proposes to issue a new system of records notice (SORN) titled, “DHS/ICE-018 Analytical Records.” DHS/ICE is creating a new system of records to better reflect and clarify the nature of all records collected, maintained, processed, and shared by ICE in large analytical data environments. A fuller description of this SORN can be found herein the Federal Register.

The DHS/ICE-018 Analytical Records system of records consolidates the following two notices, DHS/ICE-005 Trade Transparency Analysis and Research (TTAR) System of Records, 79 Fed. Reg. 71112, (December 1, 2014), and DHS/ICE-016 FALCON Search and Analysis (FALCON-SA) System of Records, 82 Fed. Reg. 20905,

(May 4, 2017), into one new system of records. This new system of records reflects the types of information and records ICE collects and maintains in analytical systems to support its law enforcement and investigative mission, rather than linking the SORN to specific IT system(s).

ICE analytical systems help ICE personnel conduct research and analysis using advanced analytic tools in support of their law enforcement and investigative mission. These tools allow ICE to query, analyze, and present large amounts of data in a variety of formats that can help illuminate relationships among the various data elements. Some analytical tools may incorporate the use of artificial intelligence and machine learning to assist ICE personnel in examining large and complex datasets. All analytical systems and tools under this system of records use a central data store to eliminate the need for multiple copies of the data.

This system of records ingests and aggregates data from a number of system and database interfaces that collect data for ICE's law enforcement, national security, immigration enforcement, and customs enforcement missions. The analytical data store also contains metadata that is created by an ICE analytical system when it ingests data. ICE uses the metadata to apply access controls and other system rules (such as retention policies) to the contents of the central data store. The metadata also provides important contextual information about the date the information was added to the data store and the source system where the data originated. ICE analytical systems also ingest external information from non-federal entities, including state and local law enforcement authorities, private corporations, or foreign governments.

The DHS/ICE-018 Analytical Records SORN also covers tips submitted to ICE via email, an online form on the ICE website, or by calling an ICE tip line phone number. These tips are created electronically using an ICE-wide tip line interface or may be

manually entered by ICE analysts. Once ICE analysts adjudicate the tips for action, the tips will then be accessible to authorized users to conduct further investigation.

Users of an analytical tool or system may create visualizations, match records, or create analyses of large volumes of data through algorithmic processes. The end result of user efforts with an analytical tool, such as a map or list, is an analytical work product. Analytical products, information sharing, and user collaboration made possible in analytical systems may result in the creation of a lead to the field.

Consistent with DHS's information sharing mission, information stored in the DHS/ICE-018 Analytical Records system of records may be shared with other DHS Components components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland security functions. In addition, DHS/ICE may share information with appropriate federal, state, local, tribal, territorial, foreign, or international government agencies consistent with the routine uses set forth in this system of records notice.

II. Privacy Act:

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which federal government agencies collect, maintain, use, and disseminate individuals' records. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, and similarly, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for

denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

The Privacy Act allows government agencies to exempt certain records from the access and amendment provisions. If an agency claims an exemption, however, it must issue a Notice of Proposed Rulemaking to make clear to the public the reasons why a particular exemption is claimed and provide an opportunity for public comment.

DHS is claiming exemptions from certain requirements of the Privacy Act for DHS/ICE-018 Analytical Records System of Records. Some information in DHS/ICE-018 Analytical Records System of Records relates to official DHS national security, law enforcement, immigration, and intelligence activities. These exemptions are needed to protect information relating to DHS activities from disclosure to subjects or others related to these activities. Specifically, the exemptions are required to preclude subjects of these activities from frustrating these processes; to avoid disclosure of activity techniques; to protect the identities and physical safety of confidential informants and law enforcement personnel; to ensure DHS' ability to obtain information from third parties and other sources; to protect the privacy of third parties; and to safeguard classified information. Disclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension.

In appropriate circumstances, when compliance would not appear to interfere with or adversely affect the law enforcement purposes of this system and the overall law enforcement process, the applicable exemptions may be waived on a case by case basis.

A system of records notice for DHS/ICE-018 Analytical Records System of Records is also published in this issue of the Federal Register.

List of Subjects in 6 CFR Part 5

Freedom of information; Privacy.

For the reasons stated in the preamble, DHS proposes to amend chapter I of title 6, Code of Federal Regulations, as follows:

PART 5--DISCLOSURE OF RECORDS AND INFORMATION

1. The authority citation for Part 5 continues to read as follows:

Authority: 6 U.S.C. sec. 101 et seq.; Pub. L. 107-296, 116 Stat. 2135; 5 U.S.C. sec. 301.

2. In appendix C to part 5, add paragraph 85 to read as follows:

Appendix C to Part 5 – DHS Systems of Records Exempt From the Privacy Act

* * * * *

85. The DHS/ICE-018 Analytical Records System of Records consists of electronic and paper records and will be used by DHS and its components. The DHS/ICE-018 Analytical Records System of Records is a repository of information held by DHS in connection with its several and varied missions and functions, including, but not limited to the enforcement of civil and criminal laws; investigations, inquiries, and proceedings thereunder; and national security and intelligence activities. The DHS/ICE-018 Analytical Records System of Records contains information that is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other federal, state, local, tribal, foreign, or international government agencies.

The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. secs. 552a(c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), (e)(8), (f), and (g). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a (k)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. secs. 552a(c)(3), (d), (e)(1), (e)(4)(G), (e)(4)(H), and (f). Where a record received from another system has been exempted in that source system under 5 U.S.C. sec. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed

for the original primary systems of records from which they originated and claims any additional exemptions set forth here.

Exemptions from these particular subsections are justified, on a case-by-case basis to be determined at the time a request is made, for the following reasons:

- (a) From subsection (c)(3) and (4) (Accounting for Disclosures) because release of the accounting of disclosures could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS as well as the recipient agency. Disclosure of the accounting would therefore present a serious impediment to law enforcement efforts and efforts to preserve national security. Disclosure of the accounting would also permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension, which would undermine the entire investigative process. When an investigation has been completed, information on disclosures made may continue to be exempted if the fact that an investigation occurred remains sensitive after completion.
- (b) From subsection (d) (Access and Amendment to Records) because access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of that investigation and reveal investigative interest on the part of DHS or another agency. Access to the records could permit the individual who is the subject of a record to impede the investigation, to tamper with witnesses or evidence, and to avoid detection or apprehension. Amendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an unreasonable administrative burden by requiring investigations to be continually reinvestigated. In addition, permitting access and amendment to

such information could disclose security-sensitive information that could be detrimental to homeland security.

- (c) From subsection (e)(1) (Relevancy and Necessity of Information) because in the course of investigations into potential violations of federal law, the accuracy of information obtained or introduced occasionally may be unclear, or the information may not be strictly relevant or necessary to a specific investigation. In the interests of effective law enforcement, it is appropriate to retain all information that may aid in establishing patterns of unlawful activity.
- (d) From subsection (e)(2) (Collection of Information Directly from Individuals) because requiring that information be collected from the subject of an investigation would alert the subject to the nature or existence of the investigation, thereby interfering with that investigation and related law enforcement activities.
- (e) From subsection (e)(3) (Notice to Subjects) because providing such detailed information could impede law enforcement by compromising the existence of a confidential investigation or reveal the identity of witnesses or confidential informants.
- (f) From subsections (e)(4)(G), (e)(4)(H), and (e)(4)(I) (Agency Requirements) and (f) (Agency Rules), because portions of this system are exempt from the individual access provisions of subsection (d) for the reasons noted above, and therefore DHS is not required to establish requirements, rules, or procedures with respect to such access. Providing notice to individuals with respect to existence of records pertaining to them in the system of records or otherwise setting up procedures pursuant to which individuals may access and view records pertaining to themselves in the system would undermine investigative efforts and reveal the identities of witnesses, and potential witnesses, and confidential informants.

(g) From subsection (e)(5) (Collection of Information) because with the collection of information for law enforcement purposes, it is impossible to determine in advance what information is accurate, relevant, timely, and complete. Compliance with subsection (e)(5) would preclude DHS agents from using their investigative training and exercise of good judgment to both conduct and report on investigations.

(h) From subsection (e)(8) (Notice on Individuals) because compliance would interfere with DHS's ability to obtain, serve, and issue subpoenas, warrants, and other law enforcement mechanisms that may be filed under seal and could result in disclosure of investigative techniques, procedures, and evidence.

(j) From subsection (g) (Civil Remedies) to the extent that the system is exempt from other specific subsections of the Privacy Act.

James Holzer,
Acting Chief Privacy Officer,
U.S. Department of Homeland Security.

[FR Doc. 2021-05643 Filed: 3/19/2021 8:45 am; Publication Date: 3/22/2021]